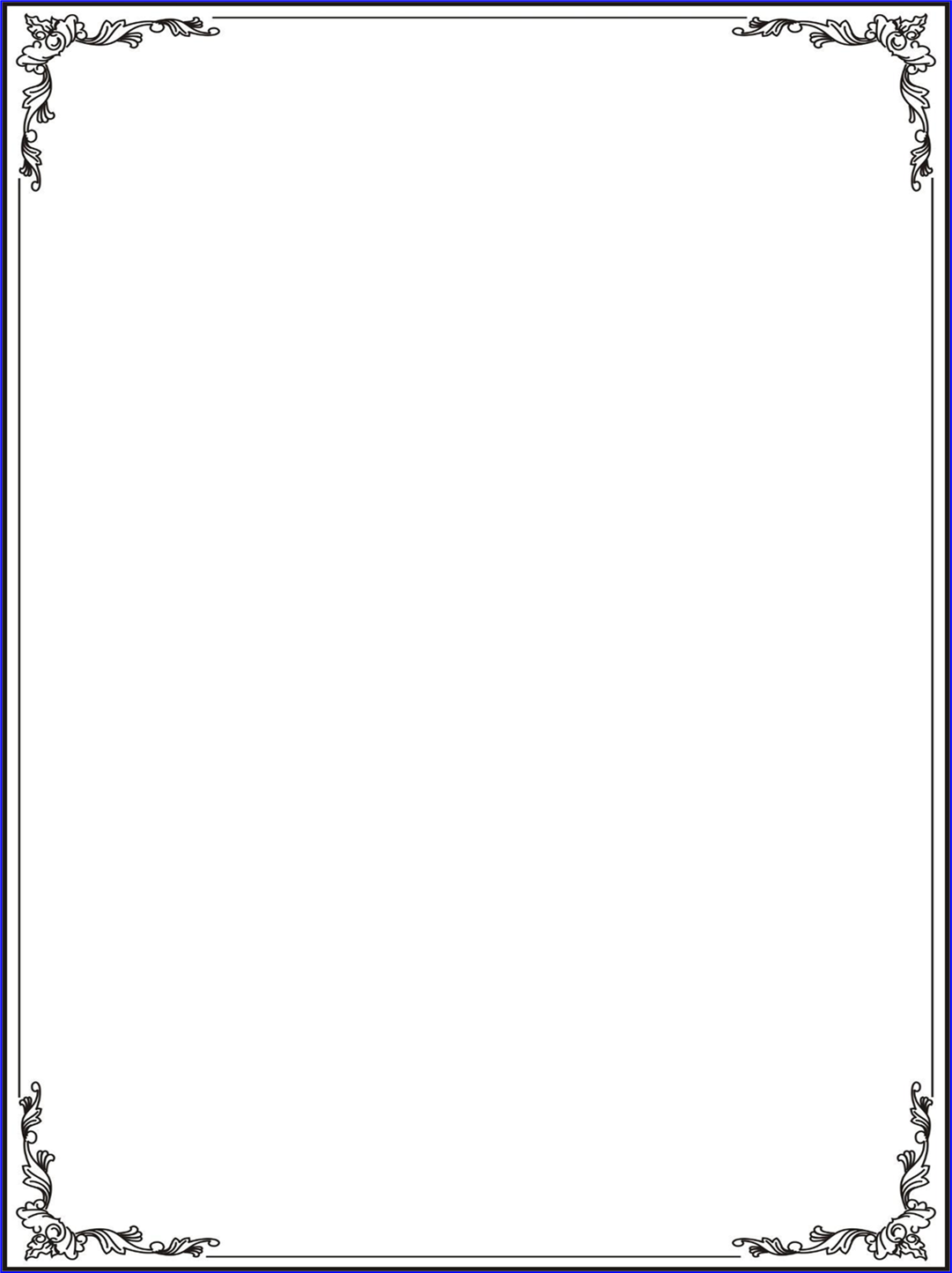
**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP.HCM**

**KHOA CÔNG NGHỆ THÔNG TIN**

**🙡🕮🙣**

****

**BÁO CÁO**

**MÔN HỌC: THIẾT KẾ MẠNG**

Đề tài

**THIẾT KẾ MẠNG CHO DOANH NGHIỆP**

**GVHD: Huỳnh Nguyên Chính**

**Mã LHP:** CNDE430780

**Sinh viên thực hiện:**

Mai Khắc Quyền 22162037

**Tp. Hồ Chí Minh, tháng 5 năm 2025**

MỤC LỤC

[**CHƯƠNG 1. THU THẬP VÀ PHÂN TÍCH YÊU CẦU DỰ** 1](#_Toc198417679)

[**1.1 Giới thiệu về công ty Brain-Rot** 1](#_Toc198417680)

[**1.2 Khảo sát và phân tích các ràng buộc yêu cầu** 1](#_Toc198417681)

[**1.2.1 Khảo sát thiết kế cần thiết cho dự án** 1](#_Toc198417682)

[**1.2.2 Mục tiêu khi thiết kế** 2](#_Toc198417683)

[**CHƯƠNG 2. THIẾT KẾ GIẢI PHÁP MẠNG LOGIC** 3](#_Toc198417684)

[**2.1 Thiết kế mạng công ty** 3](#_Toc198417685)

[**2.2 Thiết kế mạng chi nhánh** 4](#_Toc198417686)

[**2.3 Phân Hoạch Vlan** 6](#_Toc198417687)

[**2.4 Thiết kế topo mạng** 7](#_Toc198417688)

[**2.4.1 Sơ đồ vật lý** 7](#_Toc198417689)

[**2.4.2. Sơ đồ logic** 8](#_Toc198417690)

[**CHƯƠNG 3. LỰA CHỌN THIẾT BỊ** 9](#_Toc198417691)

[**3.1 Thiết bị Router** 9](#_Toc198417692)

[**3.2 Tường Lửa** 10](#_Toc198417693)

[**3.3 Switch Core** 11](#_Toc198417694)

[**3.4 Switch Access** 12](#_Toc198417695)

[**3.5 Switch Distribution** 14](#_Toc198417696)

[**3.6 Server** 15](#_Toc198417697)

[**3.7 Cáp kết nối** 17](#_Toc198417698)

[**3.8 Sơ đồ nối cáp** 18](#_Toc198417699)

[**CHƯƠNG 4. GIẢI PHÁP BẢO MẬT VÀ ĐẢM BẢO TÍNH SẴN SÀNG** 19](#_Toc198417700)

[**4.1 Bảo mật** 19](#_Toc198417701)

[**4.2 Đảm bảo tính sẵn sàng cao (High Availability)** 20](#_Toc198417702)

[**CHƯƠNG 5. DỰ PHÒNG THIẾT BỊ, ĐƯỜNG TRUYỀN VÀ NGUỒN ĐIỆN** 22](#_Toc198417703)

[**5.1 Dự phòng thiết bị** 22](#_Toc198417704)

[**5.2 Dự phòng đường truyền** 22](#_Toc198417705)

[**5.3 Dự phòng nguồn điện** 22](#_Toc198417706)

[**CHƯƠNG 6. KHẢ NĂNG MỞ RỘNG HỆ THỐNG** 23](#_Toc198417707)

[**6.1 Mô hình mạng 3 tầng rất linh hoạt:** 23](#_Toc198417708)

[**6.2 Thiết bị mạng:** 23](#_Toc198417709)

[**CHƯƠNG 7. SO SÁNH HIỆU NĂNG VÀ TÍNH NĂNG VỚI CÁC MODEL CÙNG LOẠI.** 24](#_Toc198417710)

[**CHƯƠNG 8. TỔNG CHI PHÍ** 26](#_Toc198417711)

[**CHƯƠNG 9. KẾT LUẬN** 27](#_Toc198417712)

# 

# **CHƯƠNG 1. THU THẬP VÀ PHÂN TÍCH YÊU CẦU DỰ**

## **1.1 Giới thiệu về công ty Brain-Rot**

Brain-Rot là công ty chuyên về ngành giải trí, với quy mô khoảng 100 nhân viên. Công ty tập trung phát triển các sản phẩm và dịch vụ giải trí sáng tạo, đa dạng nhằm mang đến trải nghiệm độc đáo và hấp dẫn cho khách hàng.

Để đáp ứng nhu cầu trao đổi thông tin và chia sẻ tài nguyên trong nội bộ công ty, Brain-Rot nhận thấy việc thiết kế một hệ thống mạng LAN hiện đại, có hiệu suất cao, đảm bảo tính sẵn sàng và bảo mật là cực kỳ cần thiết. Hệ thống mạng này giúp các phòng ban trong công ty kết nối và phối hợp hiệu quả, đồng thời bảo vệ an toàn dữ liệu và tài nguyên quan trọng.

## **1.2 Khảo sát và phân tích các ràng buộc yêu cầu**

### **1.2.1 Khảo sát thiết kế cần thiết cho dự án**

Có trụ sở chính đặt tại khu vực Thủ Đức, Thành phố Hồ Chí Minh, gồm các phòng ban như:

• Phòng Lễ Tân

• Phòng Kỹ thuật

• Phòng Kinh doanh

• Phòng Họp

• Phòng Giám đốc

• Phòng Kế toán

Có các máy chủ nội bộ như AD, DNS, DHCP.

Có hỗ trợ các dịch vụ như Web, Mail server.

Truy cập ra ngoài Internet

### **1.2.2 Mục tiêu khi thiết kế**

Hệ thống mạng được thiết kế nhằm đáp ứng các yêu cầu về hiệu suất, bảo mật và khả năng mở rộng, phù hợp với nhu cầu hoạt động của tổ chức. Cụ thể, mục tiêu thiết kế bao gồm:

**Hiệu suất :** Đảm bảo tốc độ truyền tải dữ liệu nhanh chóng, giảm thiểu độ trễ, hỗ trợ các ứng dụng yêu cầu băng thông lớn.

**Bảo mật:** Tích hợp các cơ chế bảo mật nhằm bảo vệ hệ thống trước các nguy cơ tấn công mạng.

**Dễ dàng quản lý:** Cung cấp công cụ quản lý tập trung, giám sát mạng theo thời gian thực, tối ưu hoá việc vận hành và bảo trì.

**Tính sẵn sàng cao:** Đảm bảo hệ thống hoạt động liên tục, có phương án dự phòng về thiết bị, đường truyền và nguồn điện để hạn chế gián đoạn dịch vụ..

**Khả năng mở rộng:** Định hướng thiết kế linh hoạt, dễ dàng nâng cấp hoặc bảo trì hệ thống khi có nhu cầu mà không ảnh hưởng đến hiệu suất chung.

**CHƯƠNG 2. THIẾT KẾ GIẢI PHÁP MẠNG LOGIC**

## **2.1 Thiết kế mạng công ty**

Mạng nội bộ công ty được xây dựng dựa mô hình mạng 3 tầng (Three-tier Network Architecture) gồm Core, Distribution và Access, đảm bảo hiệu suất, tính sẵn sàng và dễ quản lý.

1. **Lớp Core**

Tầng Core đóng vai trò là xương sống của hệ thống mạng, chịu trách nhiệm kết nối các switch phân phối (Distribution Switches) với nhau và với bộ định tuyến (router) kết nối ra Internet.

Đây là lớp cung cấp các liên kết tốc độ cao, đảm bảo lưu lượng dữ liệu lớn được xử lý hiệu quả và nhanh chóng.

Tầng Core phải đảm bảo tính sẵn sàng cao và khả năng chịu tải lớn, vì nó tập trung toàn bộ lưu lượng mạng.

Việc thiết kế dự phòng (redundancy) ở tầng này giúp tránh điểm lỗi đơn (SPOF) và đảm bảo mạng luôn ổn định khi có sự cố

1. **Lớp Distribution**

Tầng Distribution nằm giữa Core và Access, đóng vai trò tổng hợp kết nối từ các switch ở tầng Access.

Nhiệm vụ chính là định tuyến nội bộ giữa các VLAN hoặc subnet, đảm bảo lưu lượng giữa các phân vùng mạng được xử lý chính xác

Đồng thời, tầng này áp dụng các chính sách mạng quan trọng như ACL (Access Control List) để kiểm soát truy cập và QoS (Quality of Service) để ưu tiên lưu lượng cho các dịch vụ quan trọng.

Tầng Distribution cũng thường được bố trí theo từng tòa nhà hoặc nhóm phòng ban, giúp quản lý mạng phân vùng và dễ dàng mở rộng khi cần thiết.

Việc phân vùng rõ ràng giúp khoanh vùng sự cố, giảm thiểu ảnh hưởng khi một phần mạng gặp lỗi.

1. **Lớp Access**

Tầng Access là lớp kết nối trực tiếp đến các thiết bị người dùng cuối như máy tính để bàn (PC), điện thoại IP (IP Phone), điểm truy cập Wi-Fi (Access Point), camera...

Tầng này cung cấp các cổng Gigabit Ethernet tốc độ cao để đáp ứng nhu cầu truyền dữ liệu của thiết bị.

Đồng thời, tầng Access triển khai các cơ chế bảo mật truy cập mạng như xác thực 802.1X, phân VLAN, port security để kiểm soát và bảo vệ người dùng truy cập.

Khi xảy ra sự cố tại tầng Access hoặc Distribution, thiết kế phân vùng mạng giúp phạm vi lỗi được khoanh vùng, tránh lan rộng sang các phần khác của hệ thống mạng.

## **2.2 Thiết kế mạng chi nhánh**

Thiết kế mạng tại các chi nhánh được xây dựng tương tự mô hình tại trụ sở chính, với các thành phần chính như sau:

**Tường lửa (Firewall):**

Thiết bị firewall bảo vệ mạng chi nhánh khỏi các truy cập trái phép. Firewall được kết nối đồng thời với router và switch Distribution, có thể cấu hình chế độ High Availability (HA) hoặc load balancing để tăng cường bảo mật và dự phòng.

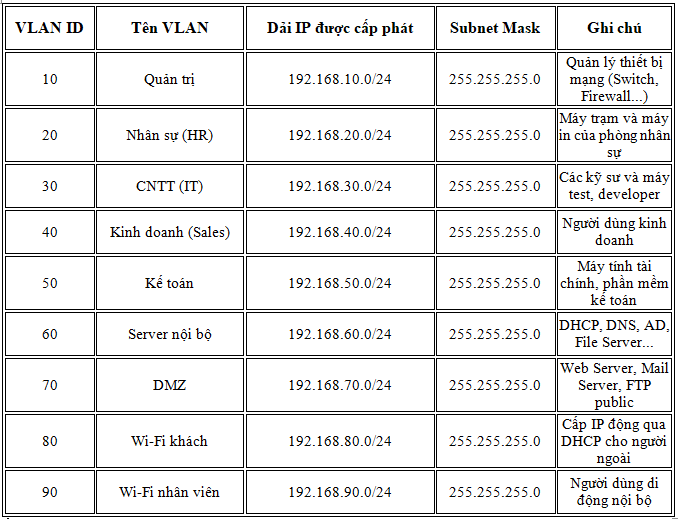
**Switch Distribution:**

Chịu trách nhiệm kết nối các switch Access trong chi nhánh với thiết bị định tuyến và bảo mật. Các switch Distribution có nhiều liên kết chéo (redundancy links) nhằm tăng cường độ tin cậy và khả năng chịu lỗi (high availability).

**DHCP Server:**

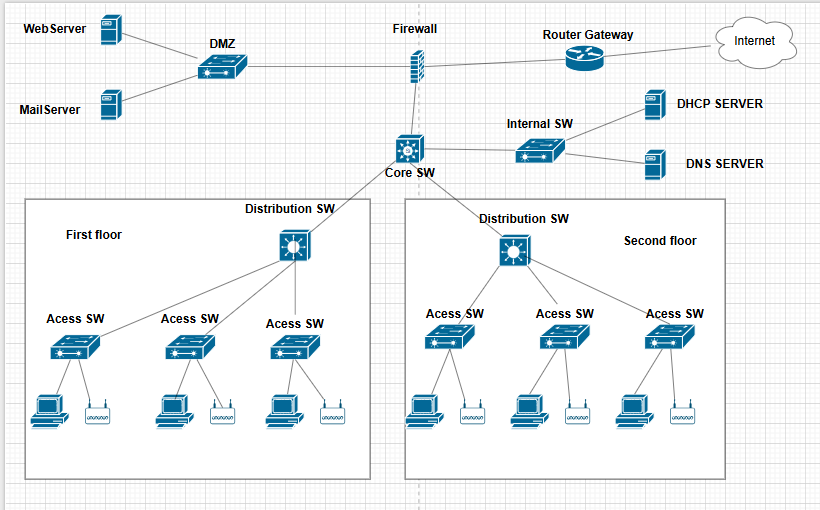
Cung cấp địa chỉ IP động cho toàn bộ thiết bị đầu cuối trong chi nhánh. DHCP Server được kết nối với switch Distribution trước khi chuyển tiếp tới các switch Access để phân phát IP, đảm bảo quản lý địa chỉ mạng tập trung và hiệu quả.

## **2.3 Phân Hoạch Vlan**



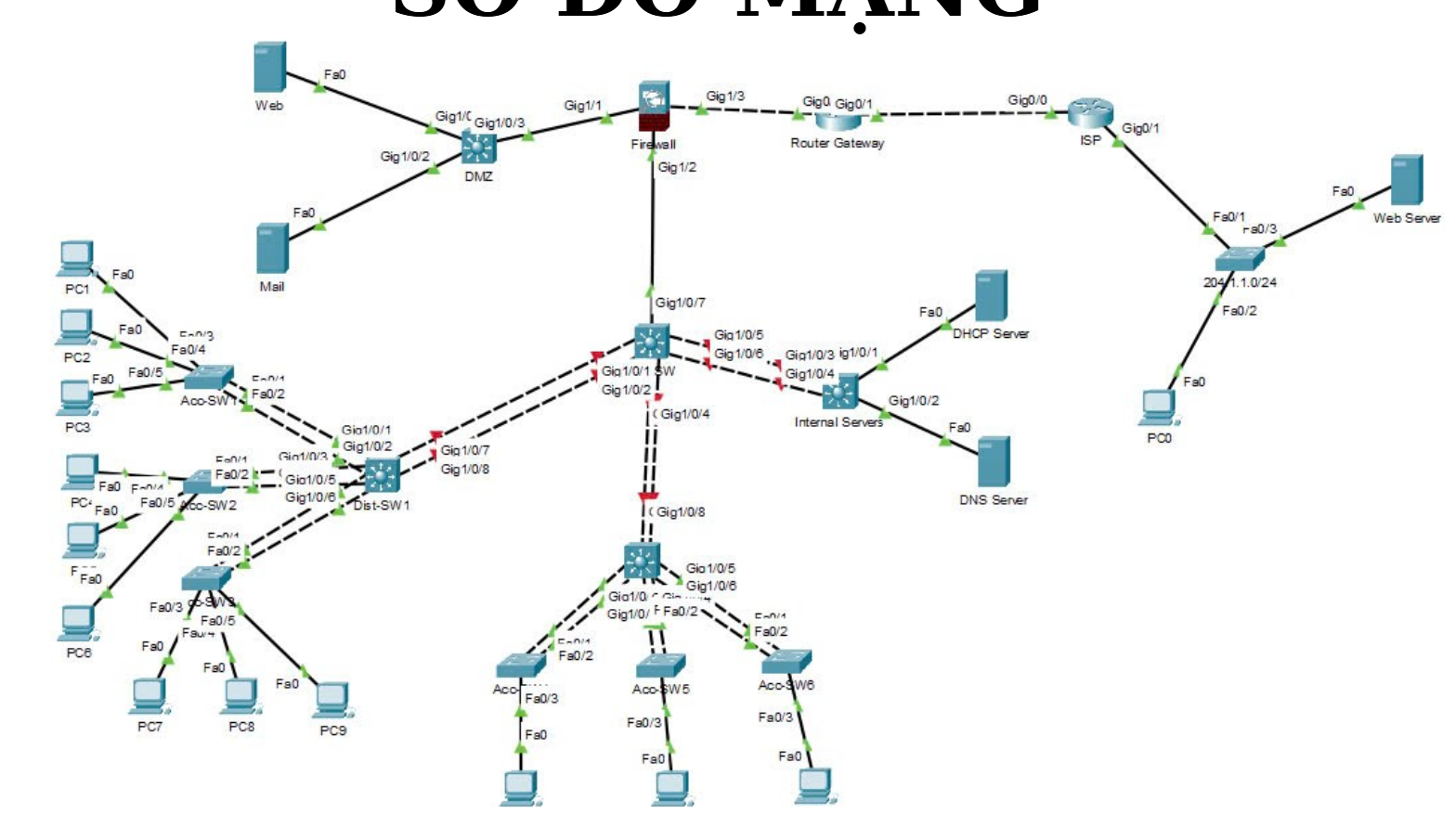
## **2.4 Thiết kế topo mạng**

### **2.4.1 Sơ đồ vật lý**

****

*Hình 1: Sơ đồ vật lý*

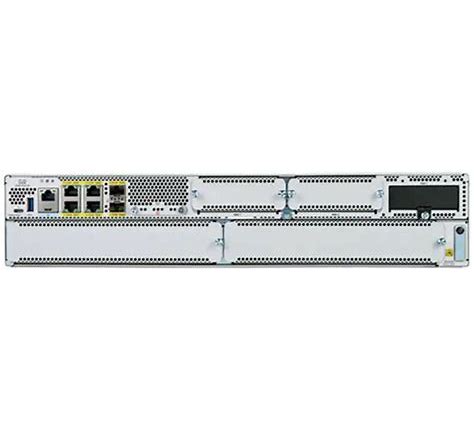
### **2.4.2. Sơ đồ logic**



*Hình 2: Sơ đồ logic*

# **CHƯƠNG 3. LỰA CHỌN THIẾT BỊ**

## **3.1 Thiết bị Router**



*Hình 3: Cisco-C8300-1N1S-4T2X*

**Thông số kỹ thuật**

* Giao diện mạng:
  + 2 cổng 10-Gigabit Ethernet SFP+.​
  + 4 cổng 1-Gigabit Ethernet RJ-45.​
  + 1 khe cắm SM (Service Module).
  + 1 khe cắm NIM (Network Interface Module).​
  + 1 khe cắm PIM (Pluggable Interface Module).
* Hiệu suất:
  + Thông lượng chuyển tiếp IPv4: lên đến 19,7 Gbps.​
  + Thông lượng IPsec với gói tin 1400 byte: lên đến 16,9 Gbps.​
  + Thông lượng SD-WAN IPsec với gói tin 1400 byte: lên đến 17 Gbps.​
  + Hỗ trợ tối đa 6.000 kênh SD-WAN Overlay.​
* License: Cisco DNA Essentials.
* Bộ nhớ và lưu trữ:
  + Bộ nhớ DRAM mặc định: 8 GB.​
  + Bộ nhớ flash: 8 GB.​
  + Lưu trữ M.2 SSD mặc định: 16 GB, có thể nâng cấp lên 32 GB hoặc 600 GB NVMe.​
* Kích thước và môi trường hoạt động:
  + Kích thước (Cao x Rộng x Sâu): 1,73 inch x 17,5 inch x 16,25 inch.​
  + Trọng lượng (với 2 nguồn AC và quạt): khoảng 9,07 kg.​
  + Nhiệt độ hoạt động: từ 0°C đến 40°C.​
  + Độ ẩm hoạt động: từ 5% đến 85% (không ngưng tụ).​
* Thiết bị này hỗ trợ nhiều giao thức mạng như Static Route, RIP, OSPF, EIGRP, BGP, IS-IS, MPLS.

## **3.2 Tường Lửa**



*Hình 3: Cisco FPR4112-NGFW-K9*

**Thông số kỹ thuật**

* Giao diện mạng:
  + 8 cổng 10-Gigabit Ethernet SFP+.​
  + 1 cổng quản lý SFP 1-Gigabit Ethernet.​
  + 1 cổng console RJ-45.​
  + 1 cổng USB 2.0.​
  + 2 khe cắm module mạng (Network Module) hỗ trợ các tùy chọn 1/10/40/100G và FTW (Fail to Wire).
* Hiệu suất:
  + Thông lượng tường lửa (Firewall throughput): 40 Gbps.​
  + Thông lượng NGFW (Firewall + AVC): 19 Gbps.​
  + Thông lượng IPS (Hệ thống ngăn chặn xâm nhập): 19 Gbps.​
  + Thông lượng VPN IPsec: 8,5 Gbps.​
  + Số lượng kết nối đồng thời tối đa: 10 triệu.​
  + Số lượng kết nối mới mỗi giây: 98.000.​Số lượng VPN peers tối đa: 10.000.​
* Bộ nhớ và lưu trữ:
  + Dung lượng lưu trữ: 400 GB SSD.
* License
  + Smart License (Cisco Smart Licensing)

## **3.3 Switch Core**



*Hình 4: Cisco Catalyst C9500-40X-A*

**Thông số kỹ thuật**

* **Giao diện mạng:**
  + Hỗ trợ 4 cổng uplink 10-Gigabit Ethernet.
  + Các cổng Gigabit Ethernet hỗ trợ kết nối các thiết bị mạng.
* **Hiệu suất:**
  + Dung lượng chuyển mạch (Switching capacity): 960 Gbps.
  + Forwarding rate: 720 triệu gói mỗi giây (Mpps).
  + Hỗ trợ định tuyến Lớp 3 với các giao thức OSPF, EIGRP, VRRP.
* **Khả năng mở rộng:**
  + Tổng số địa chỉ MAC: 64,000.
  + Số tuyến IPv4: hỗ trợ lên đến 80,000 host.
  + Số tuyến IPv6: hỗ trợ lên đến 40,000 host.
  + Hỗ trợ VLAN lên tới 4,094 VLAN IDs.
* **Tính năng bảo mật:**
  + Hỗ trợ Security ACL và QoS ACL với 18,000 mục.
  + Tích hợp MACsec-256 cho mã hóa dữ liệu bảo mật cao cấp.
  + Hỗ trợ Multicast: 32,000 IPv4 & 16,000 IPv6.
* **Bộ nhớ và lưu trữ:**
  + RAM: 16GB.
  + Flash: 16GB.
* **Tính năng tự động hóa và giám sát:**
  + Hỗ trợ Netconf, Restconf, gRPC, YANG giúp quản lý thiết bị dễ dàng.
  + Telemetry: Model-driven telemetry, sampled NetFlow.
  + Hỗ trợ SD-Access với policy-based automation và assurance.
* **Khả năng chịu tải và môi trường hoạt động:**
  + Thiết kế rack 1U, kích thước 1.73 x 17.5 x 21.52 inch, trọng lượng 11.68 kg.
  + Nguồn điện: 115-230V AC.
  + Nhiệt độ hoạt động: 0–40°C, độ ẩm 5%–90%.
  + Tuân thủ các tiêu chuẩn IEEE 802.1x, IEEE 802.3ad, SNMPv3.

## **3.4** **Switch Access**



*Hình 5: Cisco-C9300-24P-A*

**Thông số kỹ thuật**

* **Cổng kết nối:**
  + 24 cổng 10/100/1000 Gigabit Ethernet hỗ trợ PoE+ với tổng công suất cấp nguồn lên đến 445W, cung cấp tối đa 30W trên mỗi cổng.
  + Khe cắm uplink mô-đun hỗ trợ các tùy chọn:​
    - C9300-NM-8X: 8 cổng 10G
* **Hiệu năng:**
  + Dung lượng chuyển mạch: 208 Gbps​
  + Tốc độ chuyển tiếp: 154,76 Mpps​
  + Băng thông xếp chồng (Stacking): 480 Gbps với công nghệ Cisco StackWise-480, hỗ trợ tối đa 8 thành viên trong một stack.​
* **Bộ nhớ:**
  + DRAM: 8 GB​
  + Flash: 16 GB​
* **Khả năng định tuyến và bảng MAC:**
  + Số lượng địa chỉ MAC tối đa: 32.000​
  + Số lượng tuyến IPv4 tối đa: 32.000 (bao gồm 24.000 tuyến trực tiếp và 8.000 tuyến gián tiếp)​
  + Số lượng tuyến IPv6 tối đa: 16.000​
  + Số lượng VLAN hỗ trợ: 4.000​
  + Kích thước gói Jumbo tối đa: 9.198 byte​
* **Tính năng xếp chồng và nguồn điện:**
  + Công nghệ xếp chồng: Cisco StackWise-480 với băng thông xếp chồng 480 Gbps​
  + Công nghệ chia sẻ nguồn: Cisco StackPower, cho phép chia sẻ năng lượng giữa các switch trong cùng một stack.​
  + Nguồn điện mặc định: PWR-C1-715WAC cung cấp công suất tối đa 715W.

## **3.5 Switch Distribution**



*Hình 6: Dell PowerConnect 8132F*

**Thông số kỹ thuật**

* **Cổng kết nối:**
  + 24 cổng SFP+ 10Gb/1Gb​
  + 1 khe cắm mô-đun mở rộng, hỗ trợ các tùy chọn sau:​
  + Mô-đun QSFP+ 40GbE 2 cổng
  + Mô-đun SFP+ 10GbE 4 cổng
  + Mô-đun 10GBase-T 4 cổng
* **Hiệu năng:**
  + Dung lượng chuyển mạch: 640 Gbps
  + Tốc độ chuyển tiếp: lên đến 960 triệu gói tin mỗi giây (Mpps)​
  + Độ trễ: < 2,0 µs​
* **Bộ nhớ:**
  + Bộ nhớ MAC: hỗ trợ lên đến 128.000 địa chỉ​
  + Bộ đệm gói tin: 9 MB​
* Kích thước gói tin tối đa (Jumbo Frame): 9.216 byte​

**Tính năng nổi bật**

* Khả năng xếp chồng (Stacking): Hỗ trợ xếp chồng lên đến 6 switch, cho phép quản lý như một thiết bị duy nhất với băng thông xếp chồng 40Gbps.​
* Hỗ trợ Data Center Bridging (DCB): Bao gồm Priority Flow Control (PFC), Enhanced Transmission Selection (ETS), Data Center Bridging Exchange (DCBx), và iSCSI TLV, tối ưu hóa cho môi trường iSCSI và FCoE.​
* Định tuyến Layer 3: Hỗ trợ các giao thức định tuyến như RIP v1/v2, OSPF v1/v2/v3, VRRP, và các tính năng định tuyến nâng cao khác.​
* Bảo mật: Hỗ trợ IEEE 802.1x, ACLs, kiểm soát truy cập dựa trên vai trò, và các tính năng bảo mật nâng cao khác.​
* Quản lý: Giao diện dòng lệnh (CLI) tiêu chuẩn công nghiệp, giao diện web, SNMP v1/v2c/v3, và hỗ trợ LLDP-MED.​

## **3.6 Server**



*Hình 7: PowerEdge T160*

**Thông số kỹ thuật**

* **CPU :** 
  + Intel Pentium G7400
* **Bộ nhớ RAM:** 
  + 32GB x4 UDIMM DDR5, tốc độ 5600MT/s, loại C3 (phân loại hiệu năng và tiết kiệm năng lượng của Dell).
* **Ổ cứng:** 
  + 32TB SAS ISE, tốc độ 7200 vòng/phút, chuẩn 12Gbps, định dạng 512e, kích thước 3.5 inch. (ISE = Instant Secure Erase (hỗ trợ xóa dữ liệu an toàn)).
* **Lưu trữ:**
  + 2 ổ cho Hệ điều hành (Windows Server 2022) SSD HPE 960GB SATA 6G Mixed Use SFF (P40499-B21)
    - Dung lượng: 1TB/ổ
    - Lý do: Hệ điều hành cần ~100GB, SSD tăng tốc khởi động và phản hồi ứng dụng
  + 3 ổ cho Dữ liệu (RAID 5)
    - SSD HPE 1.92TB SATA 6G Read Intensive SFF (P40501-B21)
    - Dung lượng: 1.92TB/ổ
    - RAID 5: Dung lượng khả dụng ~3.84TB, chịu lỗi 1 ổ
    - Lý do: Tốc độ cao và độ bền cho DHCP/DNS (truy cập nhanh, ổn định)
* **Khe mở rộng:**
  + 2 khe PCIe 4.0:​
    - 1 khe x16 với băng thông x16, kích thước Half Height, Half Length.
    - 1 khe x4 với băng thông x4, kích thước Half Height, Half Length
* **License:**
  + RHEL, 1-2SKT, 3yr Premium Subscription,Virtual Datacenters, Digitally Fulfilled

## **3.7 Cáp kết nối**



*Hình 8: Cáp Quang OM3 LC-LC 1*

**Thông số kỹ thuật**

* Loại: Multi-mode OM3
* Đầu nối: LC - LC
* Tốc độ hỗ trợ: 1G/10G/25G
* Khoảng cách: ~300m (10G)

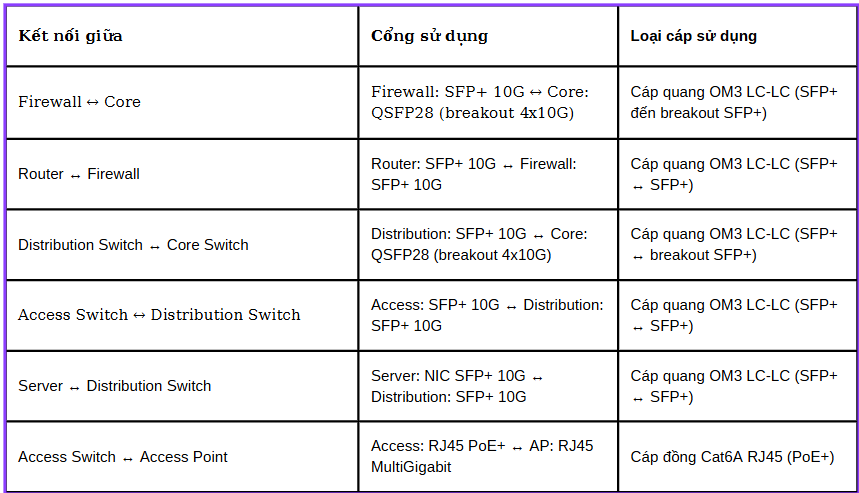


*Hình 9: Cáp Đồng Cat6A RJ45 1*

**Thông số kỹ thuật**

* Loại: Cat6A UTP, hỗ trợ PoE+
* Tốc độ: 1G/2.5G/5G
* Khoảng cách tối đa: 100m
* Dùng cho Access Switch ↔ Access Point

## **3.8 Sơ đồ nối cáp**



# **CHƯƠNG 4. GIẢI PHÁP BẢO MẬT VÀ ĐẢM BẢO TÍNH SẴN SÀNG**

## **4.1 Bảo mật**

**a. Tường lửa Cisco FPR4112-NGFW-K9:**

* Là thiết bị bảo vệ lớp biên mạng, có khả năng lọc lưu lượng, phát hiện và ngăn chặn các tấn công mạng như DDoS, malware, các truy cập trái phép.
* Hỗ trợ VPN IPsec cho các kết nối từ xa an toàn.
* Tích hợp IPS (Intrusion Prevention System) giúp chủ động phát hiện và chặn các hành vi nguy hiểm trong mạng.
* Cổng quản lý riêng biệt giúp kiểm soát và giám sát an ninh tập trung.

**b. Phân vùng mạng VLAN**:

* Hệ thống mạng được chia thành nhiều VLAN cho các phòng ban khác nhau như phòng kỹ thuật, kinh doanh, kế toán.
* Giúp cô lập các nhóm thiết bị, giảm nguy cơ truy cập trái phép nội bộ, kiểm soát lưu lượng tốt hơn.

**c. Kiểm soát truy cập (ACL)**:

* Các chính sách kiểm soát truy cập được cấu hình tại tầng Distribution và Core nhằm hạn chế truy cập trái phép giữa các VLAN hoặc subnet.
* Giúp bảo vệ các dịch vụ quan trọng như Web Server, Mail Server.

1. **Xác thực người dùng 802.1X và port security:**

* Tầng Access áp dụng xác thực chuẩn IEEE 802.1X cho phép chỉ thiết bị có chứng thực hợp lệ mới được kết nối mạng.
* Port security giới hạn số lượng thiết bị có thể kết nối vào một cổng switch, tránh việc cắm thiết bị lạ gây nguy cơ bảo mật.

1. **Mã hóa dữ liệu MACsec-256 trên Switch Core:**

* Mã hóa lưu lượng truyền giữa các switch Core để đảm bảo an toàn dữ liệu trước các nguy cơ nghe trộm, giả mạo trong mạng LAN.

**f. Giám sát mạng tập trung**:

* Sử dụng các công cụ hỗ trợ quản lý như Cisco DNA, Netconf, Restconf giúp theo dõi trạng thái thiết bị, lưu lượng, cảnh báo sớm các bất thường.

## **4.2 Đảm bảo tính sẵn sàng cao (High Availability)**

**a. Mô hình 3 tầng Core - Distribution - Access với dự phòng:**

* **Core Layer**: Cung cấp liên kết tốc độ cao, có nhiều đường truyền dự phòng liên kết giữa các switch Core và router Internet.
* **Distribution Layer**: Đóng vai trò tổng hợp, có các liên kết chéo (redundancy links) giúp chuyển hướng lưu lượng khi một liên kết hay switch bị lỗi.
* **Access Layer**: Kết nối trực tiếp đến thiết bị người dùng cuối, có cơ chế phân vùng VLAN, giúp khoanh vùng lỗi nhanh.

**b. Xếp chồng switch (Stacking):**

* Switch Access Cisco C9300 và switch Distribution Dell PowerConnect hỗ trợ công nghệ stack giúp nhiều switch hoạt động như một thiết bị duy nhất.
* Nếu một switch trong stack hỏng, các switch còn lại vẫn hoạt động bình thường, đảm bảo kết nối không bị gián đoạn.

**c. Thiết bị Router và Firewall có High Availability (HA):**

* Router Cisco C8300 và Firewall Cisco FPR4112 hỗ trợ chế độ HA với failover tự động khi thiết bị chính gặp sự cố.
* Giúp duy trì kết nối Internet và bảo mật không bị gián đoạn.

**d. Nguồn điện dự phòng:**

* Các thiết bị đều có nguồn dự phòng kép (Dual Power Supply).
* Hệ thống UPS toàn bộ phòng máy chủ và thiết bị mạng đảm bảo duy trì hoạt động khi mất điện đột ngột.

**e. Lưu trữ Server RAID 5:**

* RAID 5 cho phép chịu lỗi 1 ổ cứng mà không mất dữ liệu, tăng tính sẵn sàng cho dịch vụ lưu trữ.

# **CHƯƠNG 5. DỰ PHÒNG THIẾT BỊ, ĐƯỜNG TRUYỀN VÀ NGUỒN ĐIỆN**

## **5.1 Dự phòng thiết bị**

Thiết bị mạng (Router, Firewall, Switch Core/Distribution) được thiết kế để chạy dự phòng:

* + Router và Firewall có module dự phòng và hỗ trợ chế độ HA.
  + Switch Core và Distribution sử dụng công nghệ stack hoặc liên kết chéo giúp duy trì hoạt động khi thiết bị con hỏng.
  + Server PowerEdge sử dụng ổ cứng RAID 5, giúp tránh mất dữ liệu khi một ổ hỏng.

## **5.2 Dự phòng đường truyền**

* Mạng được thiết kế nhiều liên kết vật lý song song ở tầng Core và Distribution, tránh điểm nghẽn và mất kết nối nếu một đường truyền bị đứt.
* Sử dụng cáp quang OM3 cho các liên kết chính, đảm bảo tốc độ cao và ổn định trong truyền tải dữ liệu.

## **5.3 Dự phòng nguồn điện**

* Nguồn điện cho các thiết bị mạng đều là nguồn đôi, nếu một nguồn điện bị mất hoặc hỏng, nguồn kia tự động cấp điện.
* Hệ thống UPS tổng cho toàn bộ phòng máy chủ và các thiết bị mạng quan trọng.
* Có thể kết hợp sử dụng máy phát điện dự phòng cho các sự cố mất điện dài hạn.

# **CHƯƠNG 6. KHẢ NĂNG MỞ RỘNG HỆ THỐNG**

* 1. **Mô hình mạng 3 tầng rất linh hoạt:**
* **Core Layer**: Có khả năng chịu tải lớn, hỗ trợ mở rộng bằng cách thêm thiết bị và tăng băng thông liên kết.
* **Distribution Layer**: Có thể mở rộng theo từng tòa nhà, phòng ban, thêm switch để phục vụ nhiều VLAN và subnet hơn.
* **Access Layer**: Có thể bổ sung thêm switch Access hoặc điểm truy cập Wi-Fi mà không ảnh hưởng đến các tầng trên.
  1. **Thiết bị mạng:**
* Switch và Router đều hỗ trợ mở rộng module, stacking, và nhiều giao thức định tuyến để dễ dàng tích hợp thêm các thiết bị mới.
* Server có khe PCIe mở rộng, RAID linh hoạt, dễ dàng nâng cấp bộ nhớ, lưu trữ.

Công nghệ VLAN và định tuyến Layer 3 giúp dễ dàng thêm VLAN, subnet mới, quản lý mở rộng mạng theo nhu cầu.Các công cụ quản lý mạng hiện đại (Cisco DNA, Netconf, Restconf, YANG) giúp quản trị hệ thống mở rộng hiệu quả, tự động hóa vận hành.

# **CHƯƠNG 7. SO SÁNH HIỆU NĂNG VÀ TÍNH NĂNG VỚI CÁC MODEL CÙNG LOẠI.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Thiết bị** | **Model đã chọn** | **Lý do chọn** | **So sánh với các model khác** |
| Server | Dell PowerEdge T160 | - Cấu hình mạnh, phù hợp doanh nghiệp nhỏ. - Hỗ trợ RAID bảo vệ dữ liệu. - Giá hợp lý so với hiệu năng. | - HPE ProLiant DL20 Gen10: Mạnh hơn nhưng giá cao hơn. - Lenovo ThinkSystem ST250: Hỗ trợ RAM cao hơn nhưng không phổ biến bằng Dell. |
| Switch Core | Cisco C9600-LC-24C | - Hiệu suất cao, chịu tải lớn. - Hỗ trợ Layer 3 cho VLAN và định tuyến. - Tích hợp module quang 10G/40G. | - Arista 7050X3: Chuyên datacenter, giá cao hơn. - Juniper EX4600: Giá cạnh tranh nhưng ít tính năng SDN hơn. |
| Switch Distribution | Dell PowerConnect 8132F | - Hỗ trợ Layer 3, routing VLAN. - 24 cổng quang 10GbE, phù hợp hệ thống mạng lớn. - Giá hợp lý hơn so với các switch enterprise khác. | - HPE Aruba 8320: Hỗ trợ SDN nhưng giá cao. - Extreme Networks X460-G2: Giá mềm hơn nhưng ít tính năng hơn |
| Switch Access | Cisco C9300-24P-A | - Hỗ trợ PoE+ cấp nguồn cho AP, Camera. - Tính bảo mật cao, dễ mở rộng. | - HPE Aruba 2930F: Giá thấp hơn nhưng ít tính năng quản lý. - Juniper EX2300-24P: Giá tương đương, ít phổ biến hơn. |
| Router | Cisco C8300-1N1S-4T2X | - Hỗ trợ VPN cho nhân viên từ xa. - Hỗ trợ SD-WAN tối ưu lưu lượng mạng. | - Juniper SRX340: Tích hợp firewall nhưng ít cổng WAN. - MikroTik CCR1036: Giá rẻ hơn nhưng khó cấu hình hơn. |
| Firewall | Cisco FPR4112-NGFW-K9 | - Bảo mật mạnh, chống tấn công mạng. - Hỗ trợ phân tích lưu lượng AI. | - Fortinet FortiGate 100F: Giá mềm hơn, dễ triển khai nhưng ít tính năng nâng cao. - Palo Alto PA-3220: Bảo mật mạnh hơn nhưng giá cao hơn. |

# **CHƯƠNG 8. TỔNG CHI PHÍ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Thiết bị** | **Thông số kỹ thuật** | **Số lượng** | **Giá ước tính (USD/thiết bị)** | **Tổng chi phí (USD)** |
| Server (Dell PowerEdge T160) | Intel Xeon/Pentium G7400, 128GB DDR5, 3 HDD/SSD, RAID, Win Server 2022, SQL Std | 4 | 10.000 | 40.000 |
| Switch Core (C9600-LC-24C) | 24x QSFP28 (40/100G), SD-Access, MPLS, IOS XE, yêu cầu SUP-2 & license | 1 | 30.000 | 30.000 |
| Switch Distribution (Dell PowerConnect 8132F) | 24x SFP+ (10G), 1 slot mở rộng QSFP+, L3, OSPF/BGP, PSU 176W | 2 | 10.000 | 20.000 |
| Switch Access (C9300-24P-A) | 24x 1G PoE+, module 8x 10G SFP+, StackWise, PoE budget 437W | 7 | 5.500 | 38.000 |
| Router (C8300-1N1S-4T2X) | 2x 10G SFP+, 4x 1G RJ45, SD-WAN, VPN, DRAM 8GB, SSD 16GB | 1 | 5.000 | 5.000 |
| Firewall (FPR4112-NGFW-K9) | 8x SFP+ 10G, throughput 40Gbps, IPS 15Gbps, TLS/URL filter, 2 khe mở rộng | 1 | 30.000 | 30.000 |
| **Tổng cộng** |  |  |  | **163.000 USD** |

# **CHƯƠNG 9. KẾT LUẬN**

Dự án thiết kế mạng cho công ty Brain-Rot được triển khai bài bản, hiện đại và có định hướng phát triển lâu dài. Việc sử dụng mô hình mạng ba lớp kết hợp với các thiết bị cao cấp từ Cisco, Fortinet và HPE mang lại:

* **Hiệu suất tối ưu**: Toàn bộ mạng hỗ trợ kết nối Gigabit/10G, đáp ứng yêu cầu tốc độ cao cho các dịch vụ nội bộ và truy cập internet.
* **Bảo mật và giám sát toàn diện**: Triển khai các lớp bảo vệ như firewall, 802.1X, ACL, VLAN phân đoạn và giám sát SIEM đảm bảo an toàn cho toàn bộ hệ thống.
* **Dự phòng linh hoạt**: Từ nguồn điện, thiết bị, đường truyền đến phần mềm đều có giải pháp dự phòng, giảm thiểu rủi ro gián đoạn.
* **Khả năng mở rộng cao**: Dễ dàng bổ sung chi nhánh, người dùng, thiết bị, máy chủ và dịch vụ mới mà không ảnh hưởng đến kiến trúc hiện tại.
* **Chi phí hợp lý**: Tổng chi phí 163.000 USD phù hợp với quy mô công ty 100+ nhân sự và đảm bảo vòng đời đầu tư dài hạn.

Dự án không chỉ đáp ứng tốt nhu cầu hiện tại mà còn là nền tảng vững chắc cho các bước phát triển tiếp theo của Brain-Rot trong thời kỳ chuyển đổi số mạnh mẽ hiện nay.

# 

# **TÀI LIỆU THAM KHẢO**

1. Slide thiết kế mạng, Giáo Trình mạng căn bản - Thầy Huỳnh Nguyên Chính
2. Giáo trình Thiết kế và xây dựng mạng LAN và WAN TT khoa học tự nhiên và công nghệ quốc gia. viện công nghệ thông tin.
3. Giải pháp chuyển mạch Sisco Nexus HPT VietNam corporation
4. Cisco Service Delivery Center Infrastructure 2.1 Design Guide
5. Community College Reference Design Solution Overview
6. Community College and Vocational Education (CCVE) Design Overview